



# Department of Homeland Security Daily Open Source Infrastructure Report for 03 July 2007

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](#)

<http://www.dhs.gov/>

## Daily Highlights

- CNN reports travelers setting off for the Fourth of July holiday can expect tighter security at U.S. airports — including more police and bomb-sniffing dogs and random vehicle checks — in response to an attack Saturday on the Glasgow airport in Scotland. (See item [20](#))
- U.S. companies are increasing their scrutiny of thousands of products they receive from Chinese suppliers, as widening recalls force them to focus on potential hazards that were overlooked in the past. (See item [28](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *July 02, Associated Press* — **Checking up on power outages.** After a year of widespread and prolonged power outages due to storms, the Missouri Public Service Commission is pondering whether to adopt its most extensive rule yet governing the reliability of electricity service. The highlight, from the consumers' perspective, would be a minimum \$25 credit on monthly bills whenever it takes more than five days to restore power after a major storm or more than 16 hours during normal conditions. Much of the proposed rule focuses on the information utilities would have to collect — and report to the state — to measure their reliability. To meet the proposed rule's requirement of tracking the average number of times annually that a customer

experiences a momentary electricity outage, Ameren figures it would have to install about 8,000 automated data collection and transmission devices. The Empire District Electric projects it would cost \$8.4 million annually to comply with the rule plus \$20 million to \$30 million in equipment improvements needed to monitor its service. That nearly matches the \$25 million Empire spends yearly on poles, power lines, transformers and other equipment needed to hook up new customers, said Mike Palmer, the company's vice president of commercial operations. Source: [http://www.columbiamissourian.com/stories/2007/07/02/checkin\\_g-power-outages/](http://www.columbiamissourian.com/stories/2007/07/02/checkin_g-power-outages/)

2. *July 01, Reuters* — **IBM launches nuclear expertise center in France.** IBM will open in France its first nuclear consultancy center in July, at a time when utilities are looking to build new reactors and stretch the old ones' lifetime, an executive said. IBM is banking on a growth of the nuclear industry to increase power output to meet surging demand. Guido Bartels, IBM's global energy and utilities industry manager said that in the 30 countries with nuclear generation there was a need for sophisticated risk modeling and information tools driven by nuclear power plant license extensions and construction of new plants. But the 25-strong nuclear experts' center, he added, would be mainly focused on Europe. The full opening of EU power markets on July 1 to households was an opportunity for increased competition and increased pressure to provide cost-effective and reliable power, he added. Source: [http://www.boston.com/business/articles/2007/07/01/ibm\\_launches\\_nuclear\\_expertise\\_centre\\_in\\_france/](http://www.boston.com/business/articles/2007/07/01/ibm_launches_nuclear_expertise_centre_in_france/)
3. *June 29, Victoria Advocate (TX)* — **Nuclear plants require strict security.** Victoria, TX, would need to put in place a plan to deal with a terrorist attack on a nuclear power plant, according to a local emergency management expert in a nearby county. Victoria is the secondary site under consideration for the nuclear power plant construction. Matagorda County is the primary site for the construction. Paul Gunter of the Reactor Watchdog Project with the Nuclear Information and Resource Service said the 9/11 Commission Report showed that the terrorists' original plans were to hijack 10 airplanes, with two of those planes designated to strike nuclear power plants. Thus, plants should be protected to the minimum of what the commission's report said. After 9/11, nuclear power plants installed additional vehicle barriers in 65 sites across the nation; there are 104 reactors. The number of security officers has increased from 5,000 to 8,000 people. Personnel have received training to deal with security threats. Doug Walters, senior director of security at the Nuclear Energy Institute in Washington, said that nuclear power plants are secure and that their security has been improved. "I think, personally, a small group frontal assault on a robust facility on a nuclear plant is fairly remote," he said, "but we're ready." Source: <http://www.thevictoriaadvocate.com/233/story/81263.html>
4. *June 29, Aspen Daily News (CO)* — **Gas wells raise risk of wildfires.** The recent Cottonwood Creek Fire, which burned within 200 yards of gas wells and houses south of Parachute, CO, was a stark reminder that Western Colorado's energy industry has peppered fire-prone public and private lands with natural gas wells and pipelines. "This is a somewhat unprecedented level of gas development in this wildland setting, with not a lot of protocols established in terms of how to deal with it," said Bill Hahnenberg of the Upper Colorado River Interagency Fire Management Unit. The Upper Colorado River unit covers about four million acres and what Hahnenberg described as "a lot" of gas wells. Though there have been a few close calls with wildfires like last summer's 830-acre Red Apple Fire south of Rifle, which passed through gas

fields and caught one gas well on fire, this year is the first time that the Upper Colorado River unit has integrated energy development into its wildland fire safety plan as an "emphasis item." With the help of energy companies and the Rifle Fire Protection District, which has developed its own oil and gas response protocols, public land managers began planning firefighting protocols for wildfires in local gas fields in January.

Source: [http://www.rockymountainnews.com/drmn/local/article/0.1299.DRMN\\_15\\_5608460.00.html](http://www.rockymountainnews.com/drmn/local/article/0.1299.DRMN_15_5608460.00.html)

5. *June 29, Reuters* — **Energy firms slowly leaving New Orleans; post-Katrina decline could grow.** The boom in Gulf of Mexico oil exploration since the 1970s made New Orleans a hub of the U.S. energy industry, but the devastation caused by hurricane Katrina in 2005 has led some oil companies to move out, a mini-exodus that could grow. A recent survey by New Orleans CityBusiness magazine found that 12 of 23 publicly traded companies headquartered in New Orleans had left since Katrina, including four energy-related firms. Tidewater Inc., the world's largest operator of oil industry service vessels, recently became the latest to say it is considering moving its headquarters to Houston. Others are moving but staying closer. Chevron Corp. is leaving its downtown tower for offices in Covington, located across Lake Pontchartrain. Louisiana Offshore Oil Port also plans to relocate its offices to the north shore. The exodus is not entirely a post-Katrina trend. Mining employment, the relevant U.S. federally defined category, fell from 16,000 to 8,000 between 1990 and August 2005, before Katrina struck, said Janet Speyrer of the University of New Orleans. It has held close to 8,000 since operations resumed after Katrina, she said. And oil refining in greater New Orleans, a different U.S. federal employment category, is expected to remain strong.

Source: <http://www.canada.com/calgaryherald/news/calgarybusiness/story.html?id=1e6650a1-7aa2-45f2-b43e-6379e85a342f>

6. *June 29, Reuters* — **Playing electrical Russian roulette.** Not everybody in military-ruled Myanmar is cursing the blackouts. Thieves in the former Burma's main city, Yangon, are taking advantage of outages often lasting for more than 20 hours a day to steal the copper power cables, police said on Friday, June 29. Sometimes, of course, they get unlucky. "The thieves are risking their lives as it is impossible to know exactly when the power is going to be restored. It's just like playing Russian roulette," said one Yangon police officer. "I've seen a few cases in which thieves were electrocuted." Innocent passers-by are also falling victim. "In one case, the broken cable end left by the thief dangled into a puddle and a woman jogger was killed when she stepped into it," he said. Despite huge off-shore natural gas reserves, the southeast Asian nation's 53 million people have access to less than ten percent of the electricity per capita of neighboring Thailand.

Source: [http://today.reuters.com/news/articlenews.aspx?type=oddlyEnoughNews&storyID=2007-06-29T124828Z\\_01\\_B373271\\_RTRUKOC\\_0\\_US-MYANMAR-THIEVES.xml&WTmodLoc=NewsHome-C3-oddlyEnoughNews-2](http://today.reuters.com/news/articlenews.aspx?type=oddlyEnoughNews&storyID=2007-06-29T124828Z_01_B373271_RTRUKOC_0_US-MYANMAR-THIEVES.xml&WTmodLoc=NewsHome-C3-oddlyEnoughNews-2)

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

7. *July 01, My Fox Colorado* — **Dangerous chemicals prompt small evacuation.** A computer circuit board manufacturing building in Broomfield, CO, caught fire Sunday morning, July 1,

prompting a Hazmat team to evacuate the surrounding area to fight the fire. The blaze partially collapsed the roof and burned through stored nitric acid. Nitric acid is used in the manufacture of circuit boards and is toxic when inhaled. A nearby hotel and restaurant were evacuated. Authorities are investigating what caused the blaze at Circuits West.

Source: <http://www.myfoxcolorado.com/myfox/pages/News/Detail?contentId=3650069&version=1&locale=EN-US&layoutCode=TSTY&pageId=3.2.1>

8. *June 30, KATU (OR)* — **Chemical leaks sparks concern.** Beaverton, OR, emergency responders spent Friday afternoon, June 29, at the scene of a chemical leak at Maxim Integrated Products, a high-tech manufacturing company located at 14320 S.W. Jenkins Road. The incident began around 4:30 p.m. PDT and the chemical that leaked was silane, which is highly combustible once it is exposed to the air. Streets in the area were closed to keep people away as a precautionary measure. One person was evacuated from a nearby mobile home park.

Source: <http://www.katu.com/news/8255072.html>

9. *June 29, Naples Daily News (FL)* — **Chemical leak triggers evacuation of sports complex.** A suspected chemical leak forced the evacuation of the Immokalee Sports Complex in Immokalee, FL, on Friday, June 29, sending three employees to the hospital and shutting down the pool area until this week. Thirteen employees had to be hosed down and three were sent to the hospital for precautionary measures after a tank thought to contain a mixture of chlorine and water leaked at the park's swimming pool. But by 8 p.m. EDT, after the chemical concoction began smoking and melting the tank, authorities determined that whatever was in the tank was something other than chlorine and water. "We're not sure what it is," said Camden Smith, a spokesperson for the Collier County Public Services Division. "Whatever it is, it's eating through the tank." The complex, 505 Escambia St., was evacuated around 11 a.m. EDT due to the leak, Smith said. The leak came from a 3-year-old, 1,000 gallon tank. The tank was filled just a few days ago, Smith said. It was unclear Friday if the wrong chemical was delivered or if someone sabotaged the tank.

Source: [http://www.naplesnews.com/news/2007/jun/29/chlorine\\_leak\\_evacuates\\_immokalee\\_sports\\_complex/](http://www.naplesnews.com/news/2007/jun/29/chlorine_leak_evacuates_immokalee_sports_complex/)

[[Return to top](#)]

## **Defense Industrial Base Sector**

10. *May 31, Government Accountability Office* — **GAO-07-549: Military Operations: Actions Needed to Improve DoD's Stability Operations Approach and Enhance Interagency Planning (Report).** Since the end of the Cold War, the United States has frequently been involved in stability and/or reconstruction operations that typically last five to eight years and surpass combat operations in the cost of human lives and dollars. A 2005 presidential directive requires the Department of Defense (DoD) and State to integrate stability activities with military contingency plans. The Government Accountability Office (GAO) was asked to address (1) DoD's approach to enhance stability operations capabilities, and challenges that have emerged in implementing its approach; (2) DoD planning for stability operations and the extent of interagency involvement; and (3) the extent to which DoD is applying lessons learned in future plans. To address these issues, GAO assessed DoD policy and planning documents, reviewed planning efforts at three combatant commands, and evaluated DoD's use of lessons

learned. GAO is also conducting a related study of the Department of State's efforts to lead and coordinate stability operations. GAO recommends DoD take several actions to improve its approach to stability operations and interagency planning. DoD partially agreed with GAO's recommendations, but did not specify actions it would take to address them.

Highlights: <http://www.gao.gov/highlights/d07549high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-549>

[\[Return to top\]](#)

## **Banking and Finance Sector**

**11. *July 02, Register (UK)* — HMRC arrests ten carousel fraud suspects.** HM Revenue and Customs (HMRC) officers arrested 10 suspected multi-million pound "carousel" scammers last week in a nationwide swoop. It said arrests were made across the UK including in Birmingham, Slough, and Maidenhead, with 20 premises being searched in connection with a suspected missing trader intra community (MTIC), VAT or carousel fraud. HMRC had been investigating a group of individuals, companies, and associated bank accounts for 18 months. The results of the lengthy inquiry led to coordinated dawn raids on June 27, under the name Operation Varlet. The operation centered on the group's suspected involvement in illegally traded mobile phones using the carousel fraud method. It said mobile phones had been bought VAT-free from Europe for businesses in the UK, but that the VAT due to HMRC had been subsequently bypassed. Last month, six men were jailed for a total of nearly 48 years for their involvement in a sophisticated carousel fraud scam. Sentencing followed a huge five-year HMRC investigation that involved nearly 100 mobile phone traders. A new measure that hopes to help prevent the EU-wide scam of trading mobile phones and computer chips VAT-free was introduced in the UK on June 1 under the "reverse charge" scheme.

Source: [http://www.channelregister.co.uk/2007/07/02/hmrc\\_vat\\_carouse1\\_fraudsters/](http://www.channelregister.co.uk/2007/07/02/hmrc_vat_carouse1_fraudsters/)

**12. *July 02, Associated Press* — Bank of America completes U.S. Trust acquisition.** Bank of America Corp. said Monday, July 2, it completed its \$3.3 billion purchase of the U.S. Trust business from Charles Schwab Corp. The new entity was renamed Bank of American Private Wealth Management. The purchase vaults Charlotte-based Bank of America into a market-leading position in managing money for the rich, with some \$265 billion of private banking assets under management. Bank of America is the second largest bank by assets in the country.

Source: [http://www.nytimes.com/aponline/business/AP-Bank-of-America-US-Trust.html?\\_r=1&oref=slogin](http://www.nytimes.com/aponline/business/AP-Bank-of-America-US-Trust.html?_r=1&oref=slogin)

**13. *July 01, Associated Press* — Ohio's laptops often stolen or missing.** In Ohio, stolen or missing laptop scenarios are not unusual, according to a recent review of reports of stolen equipment by The Associated Press. Ohio Governor Ted Strickland has ordered the State Highway Patrol to review reports of stolen computer equipment following the theft of a computer backup tape earlier this month. The tape contained personal information on state employees and the names and Social Security numbers of 225,000 taxpayers. The patrol is investigating 11 reports of missing or stolen equipment this year, 26 last year and 32 in 2005, said Lt. Tony Bradshaw, an Ohio State Highway Patrol spokesperson. State agencies are not the only ones suffering thefts. In April, the Ohio House of Representatives reported three laptops



stolen from House chambers. The biggest mass theft of computers involved the 12 that were taken from a Department of Transportation office near the agency's state headquarters. Strickland recently issued an order requiring protocols for government data encryption. "You can significantly reduce the possibility of data theft by encrypting information in all of these laptops and data devices," said Keith Dailey, a spokesperson for Governor Ted Strickland. Source: [http://news.yahoo.com/s/ap/20070702/ap\\_on\\_hi\\_te/data\\_theft:\\_ylt=AnH5voVG.LD8v1CTvPaIOccjtBAF](http://news.yahoo.com/s/ap/20070702/ap_on_hi_te/data_theft:_ylt=AnH5voVG.LD8v1CTvPaIOccjtBAF)

14. *July 01, Washington Post* — **New measure to prevent fraud takes effect.** District of Columbia residents will have a new tool to fend off identity theft starting Sunday, July 1, under a new law that gives consumers the power to block access to their credit reports. The provision takes effect amid what police say is a 52 percent increase in reported identity theft cases this year. Police attribute the rise to consumers recognizing the potential for abuse and becoming more aggressive in monitoring their credit reports. The new law allows residents to place a security freeze on their reports. Loan agencies would have to get explicit permission before running checks on those consumers. A similar law will take effect January 1 in Maryland. Virginia has no law allowing freezes. In the District, police said 382 cases of identity theft were reported in the first six months of the year, compared with 248 cases for the same period in 2006. But the most common way that thieves obtain personal financial information is by combing through trash or looking in mailboxes for letters for usable information such as names and addresses, Social Security numbers, and the account numbers of credit cards and checking accounts. Source: [http://www.washingtonpost.com/wp-dyn/content/article/2007/06/30/AR2007063000890\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/06/30/AR2007063000890_pf.html)

15. *June 28, IDG News* — **MySpace again under phishing attack.** Phishers have been using compromised MySpace.com accounts to attack unsuspecting Web surfers, security experts said Thursday, June 28. The attack is thought to have infected several thousand PCs according to reports from ISPs, said Johannes Ullrich of SANS Institute. Ullrich has documented the issue on the SANS Internet Storm Center blog. Lawrence Baldwin, chief forensics officer with security vendor MyNetWatchman, discovered the threat Tuesday. Criminals have managed to install fake navigation bars on the top of MySpace.com user profile pages that, when clicked, lead to malicious computers that attempt to infect the victim's computer. The attack uses several known Internet Explorer flaws that have been fixed, so users who have installed the latest Microsoft patches are not at risk, security experts said. Two components comprise the attack. It attempts to install malicious botnet software on victims' computers, and it uses these infected computers to try to steal MySpace credentials in a phishing attack. Computers that are compromised by the attack become infected with malicious botnet software known as "flux bot," which makes them unwitting participants in the phishing scam. Source: [http://www.infoworld.com/article/07/06/28/MySpace-again-under-phishing-attack\\_1.html?source=rss&url=http://www.infoworld.com/article/07/06/28/MySpace-again-under-phishing-attack\\_1.html](http://www.infoworld.com/article/07/06/28/MySpace-again-under-phishing-attack_1.html?source=rss&url=http://www.infoworld.com/article/07/06/28/MySpace-again-under-phishing-attack_1.html)

[[Return to top](#)]

## **Transportation and Border Security Sector**

**16. July 02, USA TODAY — Britain warns of travel delays amid heightened security.**

Passengers leaving Britain's airports were urged Monday, July 2, to take subways, buses, and trains to terminals to avoid delays caused by new security measures prompted by the car-bomb terror plot. They also were warned to add extra time getting to airports because of possible delays around departure areas. The warning — from BAA, which operates many Britain's larger airports such as London's Heathrow and Gatwick — follows new, government-imposed restrictions that ban cars from approaching terminals. The restrictions prevent cars, including taxis and limousines, from using normal drop-off lanes close to departure terminals. Drop-off points have been moved away from terminals, prompting passengers to carry their bags farther to terminals. The measure is designed to avoid a repeat of Saturday's car-bomb attack on Glasgow Airport in Scotland, where a fuel-laden SUV was crashed into a departure terminal by terrorists and blown up. They also are forcing arriving passengers to walk farther to taxi stands or to pick-up points at many terminals. The drop-off measures resulted in long lines outside entrances to Heathrow on Sunday and again Monday. Heathrow is Europe's busiest airport and a big arrival and departure point for many travelers from the U.S.

Source: [http://www.usatoday.com/travel/news/2007-07-02-britain-travel\\_N.htm](http://www.usatoday.com/travel/news/2007-07-02-britain-travel_N.htm)

**17. July 02, New York Times — U.S. adds air marshals on overseas flights.** The United States is putting extra air marshals on overseas flights, particularly to and from Britain, Department of Homeland Security officials said Sunday, July 1, in one of several security measures taken in response to Saturday's attack at an airport in Scotland. The enhanced security is taking place even though Michael Chertoff, the homeland security secretary, and other top agency officials repeated Sunday that there was no credible evidence of an imminent terrorist threat to the United States. But with the approaching Independence Day holiday, they said the additional security measures were warranted, even if only to create a visible deterrence to anyone contemplating an attack.

Source: [http://www.nytimes.com/2007/07/02/washington/02homeland.html?\\_r=1&oref=slogin](http://www.nytimes.com/2007/07/02/washington/02homeland.html?_r=1&oref=slogin)

**18. July 02, WUSA9 (DC) — Metro security for July 4th.** Visitors to the National Mall will see tighter security on Metrorail this week. Hundreds of thousands of people are expected to ride the system to the annual Capitol Fourth celebration. They'll find more video surveillance and extra transit police on duty. Special detection devices will also be in use monitoring the air for chemicals and radiation. Metro officials say they will once again close the Smithsonian Station and will limit the items people can bring on the train. The system will operate at normal hours throughout the week.

Source: [http://www.wusa9.com/news/news\\_article.aspx?storyid=60348](http://www.wusa9.com/news/news_article.aspx?storyid=60348)

**19. July 02, Click2Houston.com (TX) — Passenger, 85, detained after allegedly making bomb threat.** A passenger on a Southwest Airlines flight was detained after making a bomb threat, officials told KPRC Local 2. Houston police said the 85-year-old passenger made the comment as flight 2965 to St. Louis pushed back from the gate at Houston's Hobby Airport at about 11 a.m. Monday, July 2. The pilot returned the plane to the gate and all passengers were evacuated. The man was taken into police custody. The FBI is assisting with the investigation.

Source: <http://www.click2houston.com/news/13607509/detail.html>

**20. July 02, CNN — Travelers face tighter security, possible waits.** Travelers setting off for the Fourth of July holiday can expect tighter security at U.S. airports in response to an attack

Saturday on the Glasgow airport in Scotland. The Transportation Security Administration said there would be more police and bomb-sniffing dogs at airports and that authorities would be conducting random vehicle checks. Department of Homeland Security Chief Michael Chertoff told CNN that the threat level for U.S. aviation had been at orange, or high, since last August. "And that is basically the highest level, other than what happens when you have an actual attack. We have also taken some measures, people will see, some they will not see, in increased personnel, some of them obvious, some of them plain clothes, pushing out the security perimeter, not only with respect to airports, but also mass transit and transitions as well," said Chertoff. A survey conducted by AAA predicted that about 4.7 million people planned to fly over the holiday, which stretches over two weekends, since the Fourth of July falls on a Wednesday. About 34.7 million people said they planned to drive.

Source: <http://www.cnn.com/2007/TRAVEL/07/02/us.travel/index.html>

**21. *July 01, Lincoln Journal Star (NE)* — Bicyclist cited for riding on Nebraska airport**

**runway.** Lincoln Police ticketed 39-year-old Jeffrey W. Larson for trespassing Sunday, July 1, after he rode his bicycle on to the tarmac at Lincoln Municipal Airport. A former Lincoln Police officer now working security for the Lincoln Airport Authority caught the man riding around on a runway at the airport, Police Capt. David Beggs said. When officers contacted Larson, he told them he had just left the Perkins Restaurant nearby and was trying to get to the Air Park, but had gotten lost on the way. Authorities were not sure how Larson got through airport security. John Wood, executive director of the Lincoln Airport Authority, said Larson most likely entered through the National Guard base. If that is the case, officials from the Airport Authority will have to sit down with those from the National Guard sometime soon to work out potential security flaws.

Source: <http://journalstar.com/articles/2007/07/01/news/local/doc4688403d1a38f814854208.txt>

**22. *June 29, Government Accountability Office* — GAO-07-804R: Information on Port Security in the Caribbean Basin (Correspondence).**

Referred to as our "third border," the Caribbean Basin has significant maritime links with the United States. Given these links and the region's proximity, the United States is particularly interested in ensuring that the ports in the Caribbean Basin — through which goods bound for this country's ports and cruise ships carrying its citizens must travel — are secure. Section 233 (c) of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) requires the Government Accountability Office (GAO) to report on various security-related aspects of Caribbean Basin ports. While intelligence sources report that no specific, credible terrorist threats to maritime security exist in the Caribbean Basin, the officials GAO spoke to indicated that there are a number of security concerns that could affect port security in the region. GAO's prior work on maritime security issues has revealed that the three most likely modes of attack in the port environment are a suicide attack using an explosive-laden vehicle or vessel, a standoff attack using small arms or rockets, and the traditional armed assault. Other security concerns in the Caribbean Basin mentioned by U.S. agency officials include stowaways, illegal migration, and the growing influence of Islamic radical groups and other foreign terrorist organizations.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-804R>

[[Return to top](#)]



## **Postal and Shipping Sector**

23. *June 28, News-Record (NC)* — **Suspicious package sent to North Carolina plant.** Officials locked down the Lorillard Tobacco Co. plant in Greensboro, NC, on Thursday afternoon, June 28, after the discovery of a suspicious package. Two firemen in Hazmat gear entered the building shortly after 5 p.m. EDT to test the package, which fire officials said contained an unidentified powder. The firemen emerged nearly two hours later after determining the powder was not harmful. "It may be a hoax, but obviously someone has overstepped the boundaries," Police Lt. T.L. Callicutt said. The package was addressed to an employee and arrived through the U.S. mail, police said. The powder contained inside the package worried employees enough to call police. Fire officials were brought in a short time later, and the building was locked down. "The package has been turned over to Greensboro police now, and they'll take over the investigation," said Battalion Chief T.D. Hohn of the Greensboro Fire Department.  
Source: <http://www.news-record.com/apps/pbcs.dll/article?AID=/20070628/NEWSREC0101/70628041/-1/NEWSREC0201>

[[Return to top](#)]

## **Agriculture Sector**

24. *July 01, Associated Press* — **Older farmers changing agriculture.** So many American farmers are working longer than ever before that one in four is at least 65 years old. Within the next decade those older farmers will be looking for someone to take over their operations and selling millions of acres of land. Much of that land will be merged into bigger farms with fewer people working on them. Rural communities will lose even more young people, and a few will struggle for survival. At the same time, it's becoming more costly for young people to go into farming, and many of them see that they can make a better living by leaving the rural areas. The most recent census by the U.S. Department of Agriculture, conducted in 2002, shows that the average age of America's estimated two million farmers is 55 years. Young people have been leaving rural areas since the 1950s. But many who study agriculture feel the absence of youth has reached a critical point. Six percent of all farm operators are under age 35. Two decades ago they accounted for 16 percent of farmers.  
Source: <http://www.forbes.com/feeds/ap/2007/07/01/ap3875040.html>

25. *June 30, Shreveport Times (LA)* — **Salvinia continues to choke area lakes.** A free-floating fern brought into the U.S. from Brazil, Salvinia is rapidly becoming the bane of those individuals charged with keeping Louisiana's fisheries clear of invasive plants. With no natural predators, the plant can double in size every two days under optimal growing conditions and can destroy a small pond in a matter of months. Just one plant introduced into a lake could morph into 800 plants in about a month, more than 67 million plants in two months and 4.5 trillion in four months, according to the U.S. Army Corps of Engineers. Since February 2006, giant Salvinia has been reported on eight major water bodies in northwest Louisiana. Those include Lake Bistineau, Caddo Lake, Cross Lake, Toledo Bend Reservoir and Red River. But it isn't limited to the northwest parishes. Salvinia has shown up in Atchafalaya Basin and in southeast Louisiana parishes such as Terrebonne, according to Charles Dugas, director of Wildlife and Fisheries' inland fisheries aquatic vegetation division. Areas of Giant Salvinia

have been reported to cover 96 square miles up to three feet deep on one water body.

Source: <http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20070630/NEWS01/706300360/1060/NEWS01>

[[Return to top](#)]

## **Food Sector**

**26. July 02, *Wall Street Journal* — China faces a new worry: heavy metals in the food.** For nearly two decades, Lai Mandai regularly ate and sold beans, cabbage and watermelons grown on a plot of land a short walk from a lead smelting plant in her village. Like dozens of other villagers who ate locally grown food, Lai, 39 years old, developed health problems. Lai, along with 57 other villagers, was eventually diagnosed with high levels of cadmium, a heavy metal that can cause kidney disease and softening of the bones. Runoff from the factory had contaminated the farmland and entered the food supply. A Chinese government report found that rice grown in the village contained 20 times the permitted level of cadmium. After decades of industrial pollution, some of the worst contaminants making their way into the country's food come from the soil in which it is grown. So far it hasn't been determined the extent to which tainted crops such as rice, fruits and vegetables have been exported to the U.S. Pingyang, where Lai lives, is among the so-called hot spots in China where farmland lying in the shadow of factory smokestacks or mining operations has been contaminated by heavy metals. These elements can cause a sweeping range of health problems, from brain damage to cancer.  
Source: [http://online.wsj.com/article/SB118333755837554826.html?mod=googlenews\\_wsj](http://online.wsj.com/article/SB118333755837554826.html?mod=googlenews_wsj)

**27. July 01, *Kyodo News (Japan)* — More U.S. meatpackers win approval.** The U.S. Department of Agriculture said Friday, June 29, it has approved another four meat-processing plants for beef exports to Japan, bringing the total to 39. The addition of the four plants — three in Nebraska and one in Illinois — comes after the Japanese government found no problems with them through its own inspections, the department said. Unlike other beef, exports from U.S. government-certified facilities will not be subject to Japanese re-inspection, apart from a sampling system.  
Source: <http://search.japantimes.co.jp/cgi-bin/nb20070701a1.html>

**28. July 01, *International Herald Tribune* — U.S corporations scrutinize their imports from China.** U.S. companies are increasing their scrutiny of thousands of products they receive from Chinese suppliers, as widening recalls force them to focus on potential hazards that were overlooked in the past. These corporations are stepping up their analysis of imported goods that they sell and making more unannounced visits to Chinese factories for inspections. General Mills is testing for potential contaminants that it did not look for previously, although it would not name the substances. Kellogg has increased its use of outside services that scrutinize Chinese suppliers and has identified alternative suppliers if vital ingredients become unavailable. No fatalities or serious injuries from Chinese food products have been reported in the U.S., although counterfeit Chinese glycerine has been linked to at least 100 deaths in Panama.  
Source: <http://www.ihf.com/articles/2007/07/01/business/safety.php>

[[Return to top](#)]

## **Water Sector**

29. *June 30, Associated Press* — **Efforts expand to bring sea water to nation's faucets.** On a one-acre site fronting the Brownsville ship channel is a \$2.2 million assembly of pipes, sheds, and whirring machinery — Texas' entree into making Gulf of Mexico sea water suitable to drink. The plant is a pilot project for the state's first, \$150 million full-scale sea water desalination plant slated for construction in 2010. Desalting the sea water is expensive. Current cost estimates run at about \$650 per acre foot (326,000 gallons), as opposed to \$200 for purifying fresh water. Global desalination output is relatively minute — less than 0.1 percent of all drinking water. But according to a report by Global Water Intelligence, the worldwide desalination industry is expected to grow 140 percent over the next decade, entailing \$25 billion in capital investment by 2010, or \$56 billion by 2015. While the U.S. has hundreds of plants to purify brackish ground water, sea water desalination is just getting started. Tampa Bay's \$158 million sea water desalination plant opened in March. California is hoping to get about half a million acre feet of water a year from desalination. It seems a tiny portion of the state's yearly 70 million acre feet budget.

Source: <http://www.chron.com/disp/story.mpl/ap/tx/4934485.html>

30. *June 30, Xinhua (China)* — **China adopts new drinking water standard.** China's new national standard for drinking water quality will take effect Sunday, July 1. "In some of China's cities, water supply has been contaminated and residents are threatened with unsafe water," said Zhang Chengyu, an official with the Ministry of Health. The new standard will raise the quality of tap water in terms of organism, microorganism and disinfection by bringing 71 more quality indicators into monitoring in addition to the original 35 indicators that have been used.

Source: [http://news.xinhuanet.com/english/2007-06/30/content\\_6312906.htm](http://news.xinhuanet.com/english/2007-06/30/content_6312906.htm)

[\[Return to top\]](#)

## **Public Health Sector**

31. *July 02, ABC News (Australia)* — **Superbugs entrenched in Australian hospitals.** Disease experts have warned that Australian hospitals are failing to cope with antibiotic-resistant infections and little is being done to address the problem. They say golden staph and multi-resistant staphylococcus are entrenched in Australian hospitals and drastic action is needed. Each year thousands of patients in hospitals around the country end up with golden staph infections in their blood. About one third of those are commonly known as MRSA infections. MRSA is a strain of bacteria resistant to antibiotics. Professor Peter Collignon, the director of the Infectious Diseases Unit and Microbiology at the Canberra Hospital, warns that the superbugs are a serious and growing problem. "We should be concerned, I mean there's at least probably a couple of thousand people per year who have MRSA in their bloodstream," he said. "We know a third of those die within 30 days, and I would think at least half of those infections are likely to be preventable."

Source: <http://abc.net.au/news/stories/2007/07/02/1967084.htm?section=australia>

32.

*July 02, Jakarta Post (Indonesia)* — **Eighty percent of bird flu patients in Indonesia die.**

Around 80 percent of the total 111 bird flu patients in Indonesia, between 2005 and June 2007 have died, an official said. During the period, some 90 people died of bird flu virus in the country, head of the respiratory disease of the Health Ministry's Community and Environmental Disease Eradication Fonny Silvanus said. The bird flu patients ranged from one year old to 67 years old adults.

Source: <http://www.thejakartapost.com/detailgeneral.asp?fileid=20070701173636&irec=6>

- 33. July 01, Reuters** — **Bangladesh completes emergency polio vaccination drive.** Bangladesh has completed an emergency vaccination drive to immunize two million children against polio in a southeastern region close to Myanmar, officials said on Sunday, July 1. The campaign was launched after a polio-infected child from Myanmar had travelled to Chittagong and Cox's Bazar for treatment in March. Fearing the boy might have spread the virus during his stay, Bangladeshi health officials ordered the emergency vaccination drive. Myanmar also began a vaccination campaign in early May after two polio-infected children were detected in a town in western Rakhaine, near the Bangladesh border. Bangladesh and Myanmar declared themselves free of the disease in 2000.

Global Polio Eradication Initiative: <http://www.polioeradication.org/>

Source: <http://uk.reuters.com/article/homepageCrisis/idUKDHA156500.CH.242020070701>

[\[Return to top\]](#)

## **Government Sector**

Nothing to report.

[\[Return to top\]](#)

## **Emergency Services Sector**

- 34. July 02, Wall Street Journal** — **Wireless messaging used to fight crime.** Text messaging is turning into an effective crime-fighting tool around the world. Police agencies from Beijing to Boston are encouraging citizens to use it to report crime or inform on criminals. Crime-fighting organizations, private and governmental, also have begun to use text messaging to alert people about missing persons or suspects on the loose. What's unclear is how far police agencies will go in using text messaging. Currently, messages in most U.S. anticrime programs are "opt-in," meaning they are sent only to people who sign up to participate. Technologically, it would be possible for police to broadcast text alerts to practically every cell phone in a neighborhood or region regardless of whether they opted in or not. Interest is growing among police and safety agencies in several countries in using text messaging as a general emergency warning system. In Washington, DC, Westchester, NY, and some other regions, residents can register to receive text alerts ranging from severe weather to neighborhood crime activities on their cell phones. The alerts are sent by emergency agencies. Some states and the Federal Communications Commission also are looking at ways to broadcast terrorism, crime and natural disaster alerts.

Source: [http://online.wsj.com/public/article/SB118334106678254898-wn\\_c8J8WIHt1FXcFZRHOVYUcKBXU\\_20070731.html?mod=tff\\_main\\_tff\\_top](http://online.wsj.com/public/article/SB118334106678254898-wn_c8J8WIHt1FXcFZRHOVYUcKBXU_20070731.html?mod=tff_main_tff_top)

**35. July 02, Advocate (LA) — Course helps emergency officials, deaf communicate.** The East Baton Rouge, LA, Parish Office of Homeland Security & Emergency Preparedness hosted a training event designed to help first responders and the deaf community communicate effectively during an emergency on Thursday, June 28. After struggling to glean information from television news during the 9/11 terror attacks and the D.C.-area sniper attacks, Neil McDevitt, who is deaf and also designed the course, realized that emergency communication with the deaf community needs to be streamlined. "There was no centralized form of training," said McDevitt, the national coordinator for the project. In an emergency, the deaf want an explanation why they have to evacuate a building, McDevitt said. The first impulse of emergency responders, however, is to tell people to leave, without readily clarifying why, he said. In Thursday's class, participants navigated their way through simulated emergencies, such as a bomb in an apartment building. The groups then shared their experiences and talked about difficulties they faced.

Source: <http://www.2theadvocate.com/news/8275212.html?showAll=y&c=y>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

**36. July 02, Sophos — Sophos reveals top ten Web threats for June 2007.** Sophos has revealed the most prevalent malware threats causing problems for computer users around the world during June 2007. The figures show a further sharp rise in Web-based threats. Sophos uncovered an average of 29,700 new infected Web pages every day — around 80 percent of which were located on hacked legitimate sites. The top ten list of Web-based malware threats in June 2007 reads as follows: 1) Mal/Iframe; 2) Mal/ObfJS; 3) Troj/Fujif; 4) Troj/Decdec; 5) VBS/Redlof; 6) Troj/Psyme; 7) Mal/Packer; 8) Troj/Ifradv; 8) VBS/Haptime; 10) Mal/Zlob. Iframe, which works by injecting malicious code onto Web pages, has again topped the chart, accounting for nearly two thirds of the world's infected Web pages. Earlier this month, an Iframe attack on multiple Italian Websites occurred, making headlines around the world.

Source: [http://www.sophos.com/pressoffice/news/articles/2007/07/topt\\_enjun07.html](http://www.sophos.com/pressoffice/news/articles/2007/07/topt_enjun07.html)

**37. July 01, Associated Press — Cyber attacks engulf Kremlin's critics.** A political battle is raging in Russian cyberspace. Opposition parties and independent media say murky forces have committed vast resources to hacking and crippling their Websites in attacks similar to those that hit tech-savvy Estonia as the Baltic nation sparred with Russia over a Soviet war memorial. While they offer no proof, the groups all point the finger at the Kremlin, calling the electronic siege an attempt to stifle Russia's last source of free, unfiltered information. The victims, who range from liberal democrats to ultranationalists, allege their hacker adversaries hope to harass the opposition with the approach of parliamentary elections in December and presidential elections in next March. Some independent experts agree. "A huge information war awaits Russia before the elections," said Oleg Panfilov of the Center for Journalism in Extreme Situations. The groups claim the attackers use vast, online networks of computers infected with malicious software — whose owners probably aren't aware they are involved — to paralyze or erase targeted Websites. The attacks are similar to assaults unleashed in April and early May against Websites in Estonia.

Source: [http://news.yahoo.com/s/ap/20070702/ap\\_on\\_hi\\_te/russia\\_cyber\\_war;\\_ylt=Av0\\_mH\\_egVqYX41YhyBjPfwjtBAF](http://news.yahoo.com/s/ap/20070702/ap_on_hi_te/russia_cyber_war;_ylt=Av0_mH_egVqYX41YhyBjPfwjtBAF)



## Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

**38. *July 02, Associated Press* — Pipe bomb-like device explodes at Disney.** A device similar to a pipe bomb exploded in a trash can at a remote Walt Disney World parking lot early Monday, July 2, authorities said. No one was injured and no serious damage was reported in what officials believe was an isolated incident. Orange County sheriff's deputies responded to a 12:30 a.m. EDT call from Disney. An employee heard a loud noise and saw white smoke coming from the can near the Downtown Disney shopping and entertainment district, Sheriff Kevin Beary said. "We have recovered a very crude, homemade, low-level device," Beary said. "Because of the time and location of the event, we do not believe this incident was designed to cause significant property damage or injury. We also believe this is an isolated incident." Authorities were on high alert because of the airport attack in Scotland, and attempted car bombings in London, combined with America's upcoming July Fourth holiday, Beary said. Source: [http://hosted.ap.org/dynamic/stories/D/DISNEY\\_WORLD\\_TRASH\\_CA\\_N?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/D/DISNEY_WORLD_TRASH_CA_N?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT)

[[Return to top](#)]

## **General Sector**

Nothing to report.

[[Return to top](#)]

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.